The Scottish
Government

Information Sharing Toolkit Scotland

INFORMATION SHARING TOOLKIT
SCOTLAND

For organisations involved in the protection, safety, health, education and social welfare of the people in Scotland, including statutory, private and voluntary sector organisation

Contents

1 Introduction and Purpose 3

1.1 Introduction 3

1.2 The drivers for change 3

1.3 Aims of the Tool-Kit 4

1.4 Tool-Kit as standard for Scottish public bodies 4

2 The Information Sharing Toolkit approach..5

2.1 Practitioners fora and communications. 6

2.2 Informed Decision Making 7

2.3 Granularity of the agreement model 8

2.3.1 Overarching Memorandum of Understanding (O-MOU) (optional) 8

2.3.2 Information Sharing Agreements (ISA) (mandatory) 10

2.3.3 Instructions. 12

2.4 Flexibility (pick & choose as needed) 16

2.5 Reusability (independent processing using joint Instructions) 16

2.6 Information Sharing Code of Practice 17

2.7 Templates and guidelines. 17

3 Adoption of the IS Toolkit 17

4 Formal Review 17

1 Introduction and Purpose

1.1 Introduction

The Scottish Information Sharing Toolkit is an evolution of the former SASPI (Scottish Accord on the Sharing or Personal Information 2011) and the former Gold Standard in the direction of minimising personal and non-personal information risks across organisations.

The Information Commissioner's Office has welcomed the toolkit by saying that *"initiatives which aim to help organisations conform with our statutory Code of Practice on Data Sharing are to be encouraged. This toolkit should guide data controllers towards making the correct decisions with respect to the processing of information and so lessen the risk of a significant breach taking place. This, in turn, should engender the confidence of service users whilst compliant sharing of personal information will help to make organisations more effective in their service delivery".*

1.2 The drivers for change

It is not a new requirement for parties to formally agree with each other what information is shared beyond their organisational boundaries. But now the sheer complexity of public services - which criss-cross numerous bodies in the public, private and third sectors - means that it can be easy to lose sight of the governance that is required to make such information sharing lawful and for the scope, purposes and manner of that sharing to be clearly understood by all parties and transparent to the public.

The innovations in digital technology, the insatiable demand for data that this can generate, the emerging security risks and the complex legislative environment (that can both compel and restrict bodies' sharing of data) can make the governance process bewildering. The impact of not getting the right balance between controls and information sharing can be high; such as delays and cancellations to services, confusion, and duplication of effort, undermining public trust or even physical or mental harm to individuals.

The Toolkit constitutes a framework in support of the strongest ever drive for legal, safe and confident sharing of personal information within a joint working (Public Bodies Act 2014, Scotland) context. It aims to support the public in receiving services that are coherently and collaboratively delivered and based on need, while safeguarding the information rights of the individual.

Adoption of the Toolkit across Scotland will help ensure compliance with statutory and legislative requirements for disclosing person identifiable information including the Data Protection Act 2018, the Human Rights Act 1998, the common law duty of confidentiality, and relevant professional codes of conduct. It also enables compliance with the Information Commissioner's Data Sharing Code of Practice.

1.3 Aims of the Tool-Kit

The Toolkit enables organisations who provide services which are directly concerned with the safeguarding, welfare and protection of the wider public to share personal information between them in a lawful and intelligent way.

The aim of the Information Sharing Tool-Kit is to help practitioners in public bodies in Scotland navigate their way through the process that needs completed including:

- Prior to the proposed routine sharing of personal and non-personal information taking place.
- Staff at the sharp end doing the agreed information sharing correctly.
- To ensure continuous review and improvement so that the information sharing agreements and instructions enable real-life practical processes, are an integral part of operational practice and are not theoretical tick-box exercises that are completed and then quickly forgotten.

Consistency in decision making and recording is becoming ever more important. Practitioners, faced with significant demand for new information sharing agreements, need a simple re-useable framework to aid decision making and a template to record in a consistent way what was agreed. The public also need to be able to understand, and compare information sharing agreements, in a format that is consistent, clear and concise.

1.4 Tool-Kit as standard for Scottish public bodies

This framework applies to all public sector organisations, voluntary sector organisations and those private organisations contracted to deliver relevant services to the public sector and who provide services involving the health, education, safety, crime prevention and social wellbeing of the people of Scotland. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

It is expected that all Scottish public bodies will over time use the tool-kit, as old agreements are replaced by the new framework. It complements (rather than replaces) important guidance on sharing personal data issued by the Information Commissioner's Office and builds on previous initiatives that have aimed to standardise personal information sharing agreements. The tool-kit encompasses both personal and non-personal information and takes a further step in explaining and simplifying the process.

The conditions, obligations and requirements set out in this framework, and any information sharing agreements, instructions and guidelines developed in support of it, will apply to all appropriate staff, agency workers, volunteers and other data processors working on behalf of the partner organisations including their agents and sub-contractors.

Organisations providing services to individuals or Service Users[1] within Scotland will need to process information about them. Often the information which is processed constitutes “personal information.” For the purposes of this framework, personal information is information which relates to a living individual, including their image or voice, which enables them to be uniquely identified from that information on its own or from that and / or other information available to the recipient of such information.

At times, more than one organisation may become involved in the provision of a service to an individual. This may require that relevant, minimum and appropriate personal information be shared between them and their practitioners, in order that each can deliver co-ordinated, effective and seamless services to the Service Users involved.

2 The Information Sharing Toolkit approach

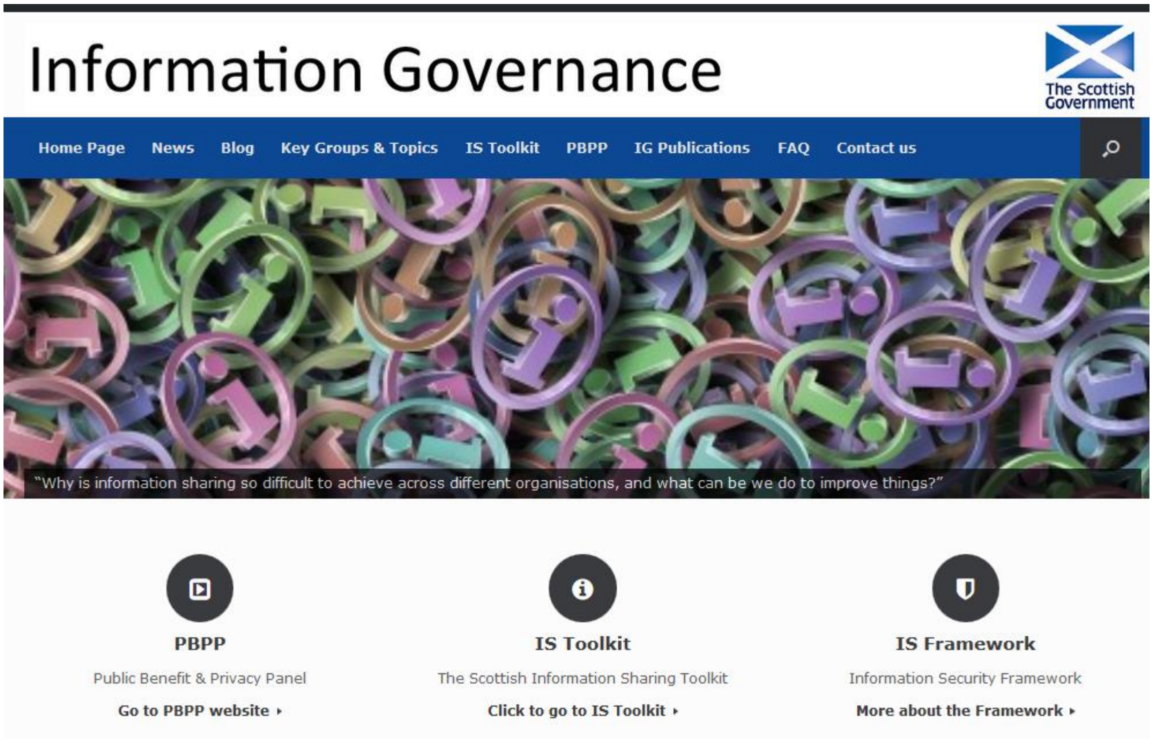
To ensure that Service Users receive the ‘seamless’, high quality support or service relevant to their needs a co-ordinated, a multi-agency approach may be appropriate. It may then be necessary for those involved to share personal information between the organisations and this requires both mutual trust and confidence in the way that each manages that information.

[1] Service Users is intended as an inclusive term to describe those people who have contact with service providing organisations within Scotland

Each organisation will acknowledge the need to comply with the requirements of codes of practice within their field of expertise and to take account of appropriate guidelines relevant to their field of work and contextual legislation.

2.1 *Practitioners fora and communications.*

In addition to using the guidance and templates, it is expected that tool-kit practitioners will develop fora and communications to share examples of good practice and methods for publishing completed information sharing agreements for others to see.



Information Governance

The Scottish Government
Home Page
News
Blog
Key Groups & Topics
IS Toolkit
PBPP
IG Publications
FAQ
Contact us

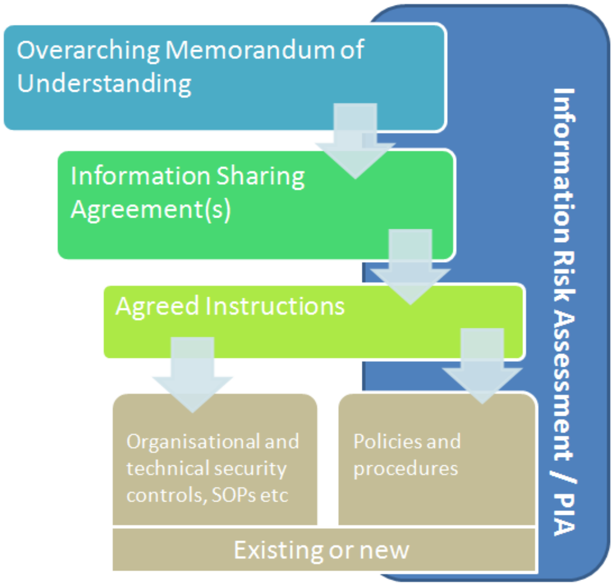
"Why is information sharing so difficult to achieve across different organisations, and what can be we do to improve things?"

PBPP
Public Benefit & Privacy Panel
Go to PBPP website ▸
IS Toolkit
The Scottish Information Sharing Toolkit
Click to go to IS Toolkit ▸
IS Framework
Information Security Framework
More about the Framework ▸

An on-line central repository of information sharing resources will be available. By self registration in the Toolkit Forum, members can also participate in discussions on specific topics of interest, upload and share relevant resources, including but not restricted to: ISAs (information sharing agreements) and underpinning work instructions, guidelines and codes of practice, information asset risk assessments and privacy notices, etc.

2.2 Informed Decision Making

The Toolkit is greatly based on the ICO Data Sharing Code of Practice. This is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. The code explains how the Data Protection Act applies to the sharing of personal data.


Overarching Memorandum of Understanding
Information Sharing Agreement(s)
Agreed Instructions
Organisational and technical security controls, SOPs etc
Policies and procedures
Existing or new
Information Risk Assessment / PIA

According to this Code of Practice, before entering into any information sharing arrangement, it is good practice to carry out a privacy impact assessment. The Information Asset Risk Assessment Template, provide a comprehensive support for undertaking the appropriate analysis of both privacy and security risks.

This will help the parties explore and discuss the benefits that the data sharing might bring to particular individuals or the public more widely. It will also help assessing any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals, as well as harm to individuals. This also allows consideration of potential harm for each of the parties entering into the agreement.

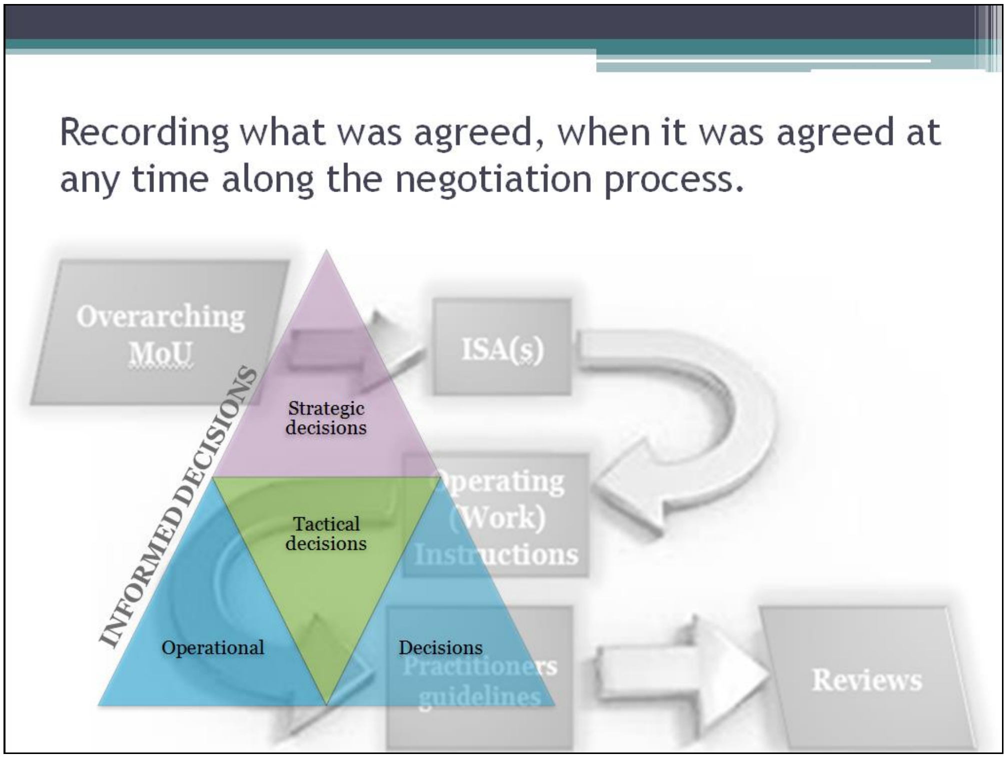
By gathering this understanding of risks, the parties can agree on specific countermeasures that may be required. This may determine the need for specific clauses in the information sharing agreement, drafting of specific guidelines, training or work instructions, or the implementation of additional security controls in all or some parts of the data sharing process.

This will also allow the parties to enter into agreements for information sharing where any residual risk is understood and to allow informed decisions within each of the parties.

2.3 Granularity of the agreement model

The Toolkit facilitates the phased recording of decisions and agreements in a progressive manner at the most appropriate time in the process. Decisions may need to be made at different stages in the agreement process, and involved different people according to the kind decisions that need to be taken.

Some agreements will cover a wide range of information sharing scenarios and complexities; the parties may recognise the benefit of the sharing and agree in principal some overarching aspects that shall facilitate future developments of more specific and contextual decisions, whilst the more detail aspects are still to be determined in later stages of the process.



Recording what was agreed, when it was agreed at any time along the negotiation process.

2.3.1 Overarching Memorandum of Understanding (O-MOU) (optional)

Some agreements will cover a wide range of information sharing scenarios, difficult to define with the level of detail required by the ICO guidelines; however, the parties may recognise the benefit of the sharing and agree in principal some overarching aspects that will facilitate future developments of more specific and contextual decisions.

Overarching Memorandums of Understanding are optional, and should be used only for the wider agreements. It will typically cover strategic decisions, for example:

- Long term aspects
- Difficult cross boundaries principles between agencies
- High risk or complex decisions
- Broader aspects of the sharing
- Strategic approach to legal liabilities between the parties

Example 1

Overarching MoU for the sharing of information within the local partnership for the integration of Health and Social Care services.

The parties joining efforts as part of the health and social care integration, may want to record their high level decisions regarding the data sharing such as:

- the scope
- the parties involved,
- the purpose for the sharing,
- the legal basis and regulatory framework in support of the sharing,
- the governance mechanisms to be put in place across the parties in order to agree on the more contextual decisions and instructions.

For this purpose, the parties can draft an overarching memorandum of understanding where only the highest level decisions are recorded. Any aspects that will be a common denominator in any underpinning information sharing agreements should also be included in the overarching MoU, e.g. if the parties have a clear position with regards to any changes to the original purposes having to be jointly agreed, and also concur that will be appropriate for the parties to have independence to proceed with any local further processing, the overarching MoU could record the conformity of the parties to move forward as data controllers in common where the purposes will be jointly determined whilst the further processing will be performed independently. The proposition that the parties will conduct the processing independently is only an example; it is a choice that requires negotiation between the parties. The MoU should reflect the agreement reached.

Recoding of these decisions, when taken at a high level and early enough in the negotiation process, should facilitate and smooth the development of the more contextual and operational decisions that need to happen at a more practical and operational level.

Overarching Memorandums of Understanding are optional, and should be used only for the wider agreements. A template is available in Appendix 1.

2.3.2 Information Sharing Agreements (ISA) (mandatory)

Any agreement for systematic sharing of information between different data controllers must be recorded in the format of an Information Sharing Agreement, regardless the existence of an overarching memorandum of understanding.

An Information Sharing Agreement sets out the common decision on the more contextual aspects of the sharing. If an overarching agreement exists between the parties covering some of the sections, is recommended to exclude them from the ISA to avoid inconsistencies, unless there is a need to record specific exceptions to matters agreed in Overarching MoUs. This will also facilitate future reviews of these agreements.

The key decisions covered in the Information Sharing Agreement are:

- the specific contextual purpose, or purposes, of the sharing
- where personal or confidential data is being shared, the legal basis for the sharing
- the potential recipients or types of recipient and the circumstances in which they will have access;
- the data to be shared;
- data quality – accuracy, relevance, usability etc;
- data security;
- any conditions which may apply / have been agreed.
- retention of shared data;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- sanctions for failure to comply with the agreement or breaches by individuals (e.g. staff) or data processors acting on behalf of the parties

The standard Information Sharing Agreement template is available in Appendix 2.

Example 1

Discharge Hub service (Hospital @ Home)

Following the same example used earlier, an Information Sharing Agreement supporting the Overarching Health and Social Care Integration MoU, would be an ISA for the sharing of information in connection with the Discharge Hub Service, which involves setting up a joint care plan for discharging of patients from hospital to home. This typically requires joint work between a number of agencies including health bodies, local authorities, and potentially third sector agencies. The ISA will detail what information can be shared, in what circumstances, and with what partners including health care professionals social work employees, and colleagues that provide other services, for example; Meals On Wheels.

ISAs are very specific and contextual whilst Overarching MoUs are high level.

Example 2

Scottish Public Pensions Agency (SPPA)

Following the same principles used earlier, an Information Sharing Agreement should be in place between all relevant parties: SPPA and employing authorities for NHS, education, police and fire service.

An Overarching Health and Social Care Integration MoU would probably not be required since the sharing of information for this purpose is very specific and unlikely to require separate negotiations at strategic and tactical level; hence the ISA along with the working instructions would suffice.

Nevertheless, if a particular territorial set of agencies decide that in their case different people have to decide very strategic matters (e.g. approach to liabilities: in common or jointly), and at a later stage a different group of people will proceed to negotiate other information sharing matters, it may be beneficial to record the more strategic agreements in a MoU (e.g. the most relevant senior stakeholders on each party agree to go ahead as Data Controllers in Common). At a later stage, a different group of people may progress the negotiations with regards to the more specific matters in the ISA (e.g. retention periods, etc.)

It makes sense a more strategic agreement (MoU) followed by the more tactical (ISA) and operational (work instructions) decisions and agreements.

The Toolkit is flexible to accommodate different scenarios. It is key to the process that negotiation that takes place at different levels (strategic, tactical and operational) at the appropriate times typically involving staff with the appropriate skills for the stage. In the simplest scenario, all the negotiation happens at once via a single ISA and a few work instructions are already in place agreed with the parties involved (e.g. their own policies and procedures).

2.3.3 Instructions.

Instructions should be seen as the interface between existing processes within the parties that need to be linked to allow the flow of information between agencies.

Example 1

Work Instructions for provisioning of user accounts

Using the same example presented in previous sections, providing access to health professionals to the social work system will require the link of existing approval processes on each partner organisation. Health care will follow its own approval path for staff requesting access to systems or data (e.g. via their line manager or head of department); once internally approved, the request has to link with the corresponding approval process in the organisation owning and managing the social work based services.

Each organisation should continue using their existing procedures whenever possible because staff are used to their "normal" working practices; a **short** work instruction describing how the parties expect to link or "bridge" their local account provisioning procedures should suffice.

It is important that linking work instructions do not overlap existing procedures in either party involved in the sharing, otherwise it could introduce inconsistencies. The IS Toolkit approach is that only exceptions and supplementary instructions should be documented in addition to any local established procedures.

Example 2

Practitioners' guidelines

Using the same illustration from earlier sections, each of the partners involved will have Work Instructions which detail the actual steps that need to be taken by practitioners when they are sharing information. The Work Instructions will include specific details, for example the name / role of relevant individuals such as authorising managers, details of the email accounts to be used if sending personal information electronically, details of which user accounts or storage mediums should be used etc.

The Work Instructions should also include details of who to contact in a potential incident or data breach, and where to go for further guidance.

Example 3

SPPA

The parties agree the SPPA Records Management Team (RMT) will manage the raw data which is submitted, however, it is agreed it remains the responsibility of the employing authority to ensure the data is fit for purpose and submitted in a format compatible with SPPA system requirement. For these submissions, a Work Instruction is prepared explaining the details of the file format, the transitions means to be used, people responsible for that operational procedure and the expected frequency or dates for submissions.

Instructions should be prepared with strong participation of the operational teams; these are staff at the sharp end of sharing the information, and should be clear on their role in the data sharing. Some additional training or awareness sessions are recommended to clarify the requirements.

Instructions typically make reference to existing policies and procedures, but new procedures or policies may also to be required for handling specific cases of information sharing or to cover gaps or discrepancies in policies across the partners.

Instructions may also be required to record agreements between the parties on specific security controls required across the partner organisations.

Due to the nature and variety of the Work Instructions, there is no standard template provided.

The following sets of instructions must exist, either in the format of joint instructions or existing documents agreed between the parties (e.g. existing local policies and procedures).

- **Sensitivity of information classification**

These instructions should cover details on the sensitivity or other classification of the information within the scope of the ISA, including whether it includes sensitive personal data as defined by the Data Protection Act 2018 Parties can agree to use classifications beyond the minimum required by legislation. Where necessary outlining where there are differences in classification between organisations and issues of equivalency (e.g. between, health, police and central government) and mapping them.

- **Controls over service users**

Controls over service users consist of agreed instructions between the parties on how the information covered by the ISA will be used only by the designated service users for the agreed purposes (e.g. role based access on systems and whether there are enhanced checks/pre-employment screening) and how these users will be designated, authorised, monitored and de-authorised as required. Access to personal data or business confidential information should be based on strict need-to-know basis.

- **Controls over information handling prior and during transmission**

These are a set of agreed instructions, policies, controls and security operating procedures which detail on how information is jointly or independently stored and then prepared for sharing, the mechanisms by which the information is to be shared (e.g. email or file-sharing protocol, tracked mail etc.) and the controls around it (e.g. encryption, tracked mail). If data is to be shared digitally also reference if any shared ICT wide area network is to be used (e.g. Scottish Wide Area Network (SWAN) or Public Services Network (PSN)) and controls needed to safe-guard confidentiality, integrity and availability of information.

- **Controls over information handling after transfer**

These controls record and manage how the recipients of the information will then process, store, delete the information which originated from outside the organisation. Note: once an organisation has shared its information externally with another data controller it often has little or no actual control over how the partner organisation then stores or uses the data. The ISA and instructions are a means of obtaining some assurance here (but ultimately it is the Data Controller who is responsible).

- **Maturity level of security in organisations sharing information**

This instruction details information about the maturity level of security in the organisations and any equivalency (e.g. both parties have data centres certified to ISO-27001; HMG Security Policy Framework; NHSS Information Security Policy Framework; both parties signed up to PSN Code of Connection etc.) and the agreed procedures to assess this maturity, monitor and communicate changes on the maturity status between the parties.

- **Relevant information security and handling policies and procedures**

All relevant security policies for the information that is to be shared should be listed in the relevant appendix of the ISA (Appendix 1 List of Instructions). Note: participating organisations may have very different policies (e.g. social media, email, online tools, devices etc.) so it will need to be agreed which operating instructions should be used and to document any agreed “bridge” or mapping instructions between local procedures and policies.

- **Audit trails and accountability**

These are instructions detailing controls on how the information sharing activities are covered by any audit trails that can identify a) which party carried out the activity such as viewing or modifying data; b) non-repudiation in event of a negative event and c) any monitoring to establish and success and security of the information sharing operations.

- **Incidents and reporting**

These consist of a description of the mechanism by which incidents and issues are reported in regard to the information within scope of the ISA (e.g. to a designated person for one or all of the parties etc.). It is also important to specify the circumstances where there needs to be external reporting (e.g. regulators such as Information Commissioner’s Office in the case of personal data; the Scottish Government or other organisation with oversight).

- **Relevant information and record management policies and procedures**

This includes the records management policies and procedures relevant to the information being shared under the ISA. The instructions will identify the retention schedule of the partner organisation and how this will be deployed (for example manual or automatic) and any mechanisms which are in place for archiving or transfer of records to other bodies for example the National Records of Scotland. In scenarios where data controllers access a pool of shared information it is important to specify retention schedules which meet the legislative and business requirements of the organisations involved.

- **Access to information legislation, intellectual property and compliance**

This refers to additional instructions or details beyond the agreements expressed in section 11 of the ISA, e.g. local procedures on how each relevant party deals with Subject Access Requests (in accordance with DPA), Freedom of Information (Scotland) Act 2002 (and subsequent amendments) or Environmental Information (Scotland) Regulations 2004 (and subsequent amendments) information requests will be managed by the parties in accordance with the processes of the relevant organisation. (For example a request for information created by National Health Services Scotland (NHSS) and then shared with a local authority is likely to managed, in the first instance, by NHSS). If Intellectual property rights or copyright are relevant, describe whether access to shared information carries any obligations to the originator / owner of that information.

2.4 Flexibility (pick & choose as needed)

Partner organisations must determine the combination of O-MoU, ISAs and Work Instructions that are required to manage and record the information sharing decisions and agreements made between the parties.

For any systematic (i.e. regular and planned) information sharing the minimum requirement is an Information Sharing Agreement and, in most cases, the corresponding Work Instructions.

Overarching MoUs are complementary to ISAs, they provide the required flexibility in the variety of negotiations that need to happen between the parties, but are optional.

2.5 Reusability (independent processing using joint Instructions)

As discussed in previous sections, Work Instructions typically make reference to existing policies and procedures and are meant to link existing processes in order to allow the flow of information across the sharing parties.

In this sense, Work Instructions should reference existing documentation as much as possible, rather than duplicating or reinventing operational procedures and policies.

It is the IS Toolkit approach to re-use existing local procedures and polices as much as possible and keep changes and exceptions to the minimum, but “bridging” processes between the parties rather than changing working practices.

The IS Toolkit Forum offers also a space for sharing experiences and resources across joining organisations, so work instructions, agreements and guidelines can be adopted or adapted by other organisations.

2.6 Information Sharing Code of Practice

Compliance with complementary Codes of Practice may be applicable for specific professional fields or contextual legislation, but in general terms, this framework endorses the ICO Data Sharing Code of Practice. This is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. The code explains how the Data Protection Act applies to the sharing of personal data. Further information is available here:

https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The ICO Publishes Data Sharing Check lists on their website, these are available here:

https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf

2.7 Templates and guidelines.

A range of guidance documents and templates have been developed to assist partner organisations in adopting the Toolkit; this resources are available on the IS Toolkit website (http://www.informationgovernance.scot.nhs.uk/).

3 Adoption of the IS Toolkit

Formal adoption of the IS Toolkit is the responsibility of the Chief Executive or Chief Officer of either a statutory body or a private or voluntary sector organisation.

Organisations that agree to support the adoption, dissemination, implementation, monitoring and review of this IS Toolkit, are invited to sign up to the IS Toolkit Forum.

Further assistance regarding adoption of the IS Toolkit, local training and awareness sessions or access to the IS Toolkit Forum can be sought from the eHealth Information Assurance & Governance Team at The Scottish Government.

4 Formal Review

This Toolkit will be reviewed every four years or as legislation dictates, by the appropriate national review group.

Overarching MoUs and Information Sharing Agreements are subject to local review by partner organisations and should be conducted at least every 2 years.

Instructions are also subject to local review by partner organisations. Appropriate review periods must be agreed between the partner organisations.